



642-627^{Q&As}

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.lead4pass.com/642-627.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Select and Place:

Click and drag the IPS terminology on the left to the correct description on the right.

false positive	A security control did not act because no malicious activity occurred.
false negative	A security control did not act when malicious activity occurred.
true positive	A security control acted when malicious activity occurred.
true negative	A security control acted when malicious activity did not occur.

Correct Answer:

Click and drag the IPS terminology on the left to the correct description on the right.

	true negative
	false negative
	true positive
	false positive

QUESTION 2

What must be configured to enable Cisco IPS appliance reputation filtering and global correlation?

- A. DNS server(s) IP address
- B. full sensor based network participation
- C. trusted hosts settings
- D. external product interfaces settings

Correct Answer: A



http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/ime/ime_collaboration.html

Global Correlation Requirements

Global correlation has the following requirements:

Valid license

You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted.

Once you install a valid license, the global correlation features are reactivated.

Agree to network participation disclaimer

External connectivity for sensor and a DNS server

The global correlation features of IPS 7.0 require the sensor to connect to the Cisco SensorBase Network.

Domain name resolution is also required for these features to function. You can either configure the sensor to connect through an HTTP proxy server that has a DNS client running on it, or you can assign an Internet routable address to the

management interface of the sensor and configure the sensor to use a DNS server. In IPS 7.0 the HTTP proxy and DNS servers are used only by the global correlation features.

QUESTION 3

Which three of these are true with respect to the numeric values associated with the target value rating? (Choose three.)

- A. Mission Critical = 100
- B. Mission Critical = 200
- C. High = 75
- D. Medium = 50
- E. Low = 75
- F. 100 is the default target value rating

Correct Answer: BEF

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html

QUESTION 4

The Cisco IPS appliance anomaly detection signatures cover which three protocols? (Choose three.)

- A. TCP



- B. ICMP
- C. UDP
- D. NETBIOS
- E. IP
- F. other

Correct Answer: ACF

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_anomaly_detection_s.html#wp2040302

Anomaly Detection Signatures

The Traffic Anomaly engine contains nine anomaly detection signatures covering three protocols (TCP, UDP, and other).

QUESTION 5

Which four networking tools does Cisco IME include that can be invoked for specific events, to learn more about attackers and victims using basic network reconnaissance? (Choose four.)

- A. ping
- B. traceroute
- C. packet tracer
- D. nslookup
- E. whois
- F. nmap

Correct Answer: ABDE

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/ime/ime_getting_started.htm | IME also supports tools such, as ping, trace route, DNS lookup, and whois lookup for selected events

[Latest 642-627 Dumps](#)

[642-627 Study Guide](#)

[642-627 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.